UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,405	05/15/2006	Aviv Abramovich	1893/47	1416

7590 08/19/2008

Mark M Friedman
c/o Polkinghorn
9003 Florin Way
Upper Marlboro, MD 20772

EXAMINER	
WANG-HURST, KATHY W	

ART UNIT	PAPER NUMBER
4173	

MAIL DATE	DELIVERY MODE
08/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/579,405	ABRAMOVICH, AVIV	
	Examiner	Art Unit	
	KATHY WANG-HURST	4173	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-10, and 12-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Barnes et al. (US 6711147)**, herein after referred as Barnes, in view of **Greis (US 2004/0028034),** further in view of **Albert Dobson (US 2005/0130645)**.

Regarding claim 1, Barnes discloses a method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including a

serving interface **(Fig. 4 items 264 and 282)** operatively

connected to the serving node **(Fig. 4 item 254)**, a gateway interface operatively connected to the gateway node **(Fig. 4 item 284)**, a processor **(col. 4 lines 13-18, IP security process, therefore must have a processor to process)** and a memory **(col. 15 line 23 and line 30)**,

wherein the data packets and the signal packets pass through said serving interface and said gateway interface **(Fig. 4),** wherein said mobile network security system monitors **(col. 4 lines 13-18 tunneling security)** the

creation **(col. 4 lines 36-41, creating tunnel)**, updating **(col. 13 lines 42-43 update tunnel)** and destruction of the tunnel **(col. 15 lines26-33 IP tunnel for a predetermined period of time therefore tunnel is destructed after predetermined time)** by monitoring the signal packets;

(b) reading by a processor the reference to the protocol context of at least one of said data packets (**col. 4 lines 13-18 use security parameters index for identifying security context, therefore read by a processor the reference to protocol context)**;

Barns fails to teach step (c). **Greis** teaches policy control function which performs applying a policy based on a tunnel profile **([0025] tunnel profile such as QoS; [0026] apply a policy)**, thereby performing at least one action to said at least one of the data packets, wherein said tunnel profile is selected based on at least one of the identifiers carried in the protocol context **([0025] distribution of packets based on TFT parameters which are included in protocol context as indicated in [0029])**.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the steps taught by Greis into the method disclosed by Barnes in order to further improve the security system by applying specific policy based on the context setting.

Greis fails to teach performing action based on the payload. Albert Dobson teaches a network monitoring method and system which identifies data packets from IMSI/phone number in the payload **([0137])** which has one or more associated PDP addresses **([0138])**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the feature taught by Albert Dobson into the step disclosed by Barn and Greis in order to further enhance the security system by applying security policies based on specific user profile embedded in the payload.

Regarding claim 2, Barnes discloses the method, according to claim 1, further comprising the step of prior to said applying:

(d) storing in said memory a tunnel context based on the protocol context, wherein said tunnel context includes said at least one of the identifiers **(col. 15 lines 30 memory; col. 13 lines 40-49 updating protocol context therefore there must exist a database to store information)**.

Regarding claim 3, Barnes discloses the method, according to claim 1, further comprising the steps of,

prior to said applying:

(d) storing said tunnel profile in said memory**(col. 15 lines 30 memory; col. 13 lines 40-49 updating protocol context therefore there must exist a database to store tunnel profile)**.

Regarding claim 4, Barnes discloses the method, according to claim 1, wherein said at least one of the

identifiers is selected from the group consisting of an access point name, a user name and a telephone number for each of the mobile stations **(col. 3 lines 1-3)**.

Regarding claim 5, Barnes discloses the method, according to claim 2, further comprising the steps of:

(e) updating said tunnel context based on at least one change of the

protocol context, and storing a modified tunnel context**(col. 13 line 40-49)**; and

(f) updating said tunnel profile based on said modified tunnel context **(col. 13 line 40-49)**.

Regarding claim 6, Barnes discloses the method, according to claim 1**(col. 13 line 40-49)**, but fails to teach the method wherein said tunnel profile is

further based on information from an external data base. **Greis** teaches an external database **([0030] and Fig. 1 item 20 BC)** for billing purposes. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was

made to incorporate external database taught by Greis into the method disclosed by Barnes in order to enhance the security system by performing additional functions such as billing.

Regarding claim 7, Barnes discloses the method, according to claim 6, but fail sto disclose the method wherein said external data base is
included in an external system selected from the group consisting of fraud management systems, charge and billing systems, account management and authentication servers**.** **Greis** teaches an external database **([0030] and Fig. 1 item 20 BC)** for billing purposes. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate external database taught by Greis into the method disclosed by Barnes in order to enhance the security system by performing additional functions such as billing.

Regarding claim 8, Barnes discloses the method, according to claim 1 **(col. 4 lines 28-41)**, but fails to disclose the method wherein said applying a policy
provides a service selected from the group consisting of security checking, bandwidth management, quality of service, virtual private network, extended security checking, intrusion detection and prevention, and voice over Internet protocol, wherein said service is selected based on said tunnel profile. **Greis** discloses a policy control function applying a policy provides a service selected from the group consisting quality of service

([0025]), security functions **([0020]),** and voice of IP **([0004]).** Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to enhance the security system by providing additional services based on the tunnel profile.

Regarding claim 9, Barnes discloses the method, according to claim 8 **(col. 4 lines 28-42)**, but fails to disclose the method wherein said service is differentiated respectively to each of the mobile stations based on said tunnel profile. Greis teaches a policy control function that treats packets differently based on tunnel profile **([0025])**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the method taught by Greis into method disclosed by Barnes in order to enhance the security system by providing difference services based on tunnel profile.

Regarding claim 10, Barnes discloses a method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transfer6ng data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further

communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including an interface to the mobile data network **(Fig. 4 item 64 security gateway)**, a processor **(col. 4 lines 13-18, an IP security process, therefore must have a processor to process)** and a memory**(col. 15 line 23)**,

wherein said mobile network security system monitors the creation**(col. 4 lines 36-41, creating tunnel)**, updating**(col. 13 lines 42-43 update tunnel)** and destruction**(col. 15 lines26-33 IP tunnel for predetermined time therefore tunnel is destructed after predetermined time)** of the tunnel by monitoring the signal packets,

(b) reading by a processor the reference to the protocol context of at least one of said data packets (**col. 4 lines 13-18 use security parameters index for identifying security context, therefore read by a processor the reference to protocol context)**;

Barnes fails to disclose (c). **Greis** teaches a security function which performs querying by a management system for information stored in the protocol context **([0025] an indicator instructing data traffic based on PDP context, which is an equivalent of a management system querying information in the protocol context)**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the

invention was made to incorporate the steps taught by Greis into the method disclosed by Barnes in order to further improve the security system by sending data packets based on protocol context.

Regarding claim 12. Barnes discloses a system which provides security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein the protocol context of the tunnel is communicated by at least one of the signaling packets, the system comprising:

(a) a serving interface operatively connected to the serving node **(Fig. 4 item 264)**;

(b) a gateway interface operatively connected to the gateway node **(Fig. 4 item 282)**;

wherein the data packets and signaling packets pass through said serving interface and said gateway interface;

Barnes fails to disclose step (c). Greis teaches a security system a processor which reads the reference to the protocol context of at least one of said data packets **([0025])**;

and

(d) a memory mechanism;

wherein said processor selects a policy based on a tunnel profile previously stored with said memory mechanism, said processor thereby performs at least one action to said at least one of the data packets, wherein said tunnel profile is selected based on at least one of the identifiers carried in the protocol context**([0025])**.

Greis fails to teach performing action based on the payload. Albert Dobson teaches a network monitoring method and system which identifies data packets from IMSI/phone number in the payload **([0137])** which has one or more associated PDP addresses **([0138])**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the feature taught by Albert Dobson into the step disclosed by Barn and Greis in order to further enhance the security system by applying security policies based on specific user profile embedded in the payload.

Regarding claim 13, Barnes discloses the system, according to claim 12, wherein said memory mechanism further stores a tunnel context based on the protocol context, wherein said tunnel context includes said at least one of the identifiers **(col. 2 line 54-col. 3 line 3)**.

Regarding claim 14, Barnes discloses the system, according to claim 12 (col. 4 lines 28-42), but fails to disclose the system further comprising:

(e) a management interface, operatively connected to a management system for querying information stored in the tunnel context. Greis teaches a billing interface **(Fig. 1 item 20)**, which is operatively connected to PFC(Fig. 1 item 19) for managing/querying billing information of the users. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate a management interface taught by Greis into the system disclosed by Barnes in order to enhance the security system by introducing a management interface to perform additional functions.

Regarding claim 15, Barnes discloses the system, according to claim 12, wherein said at least one of the identifiers is selected from the group consisting of an access point name, a user name and a telephone number of said mobile station **(col. 3 lines 1-3).**

Regarding claim 16, Barnes discloses the system, according to claim 13, wherein said processor updates said tunnel context based on at least one change of the protocol context, and thereby stores with said memory mechanism a modified tunnel context, and said processor updates said tunnel profile based on said modified tunnel context **(col. 2 line 54-col. 3 line 3)**.

Regarding claim 17, Barnes discloses the system, according to claim 13, wherein said processor updates said tunnel context based on the mobile station roaming to a second

serving node**(col. 2 line 54-col. 3 line 3)**.

Regarding claim 18, Barnes discloses the system, according to claim 13, wherein said processor destroys a tunnel context by commanding at least one node selected from the group consisting of serving nodes and gateway nodes to destroy the tunnel **(col. 15 lines 26-32)**.

Regarding claim 19, Barnes discloses the system but fails to disclose, according to claim 12, further comprising:
(e) an external database, wherein said tunnel profile is further based on information from said external data base. **Greis** teaches an external database **([0030] and Fig. 1 item 20 BC)** for billing purposes. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate external database taught by Greis into the method disclosed by Barnes in order to enhance the security system by performing additional functions such as billing.

Regarding claim 20, Barnes discloses the system, according to claim 19, but fails to disclose the system wherein said external data base is included in an external system selected from the group consisting of fraud management systems, charge and billing systems, account management systems and authentication servers. **Greis** teaches an external database **([0030] and Fig. 1 item 20 BC)** for billing purposes. Therefore, it

would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate external database taught by Greis into the method disclosed by Barnes in order to enhance the security system by performing additional functions such as billing.

Regarding claim 21, Barnes discloses the system, but fails to disclose according to claim 12, wherein said policy provides a service selected from the group consisting of security checking bandwidth management, quality of service, virtual private network, extended security checking, intrusion detection and prevention and voice over Internet protocol; wherein said
service is selected based on said tunnel profile; wherein said service is differentiated respectively to each of the mobile stations based on said tunnel profiles. **Greis** discloses a policy control function applying a policy provides a service selected from the group consisting quality of service **([0025])**, security functions **([0020]),** and voice of IP **([0004]).** Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to enhance the security system by providing additional services based on the tunnel profile.

Regarding claim 22, Barns discloses aA method for providing security during roaming and handoff from a first mobile data network to a second mobile data network, each

network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including" a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a first mobile network security system to the first mobile data network and further providing a second mobile network security system to the second mobile data network, each security system including a serving interface operatively connected to the serving node **(Fig. 4 item 264)**, a gateway interface operatively connected to the gateway node **(Fig. 4 item 282)**, a processor **(col. 4 lines 13-18, an IP security process, therefore must have a processor to process)** and a memory **(col. 15 line 23)**,

wherein the data packets and the signal packets pass through said serving interface and said gateway interface, wherein said first and second mobile network security system monitor the creation **(col. 4 lines 36-41, creating tunnel)**, updating **(col. 13 lines 42-43 update**

tunnel) and destruction **(col. 15 lines26-33 IP tunnel for predetermined**

time therefore tunnel is destructed after predetermined time) of the tunnel by monitoring the signal packets,

(b) reading by a processor the reference to the protocol context of at least one of said data packets (**col. 4 lines 13-18 use security parameters index for identifying security context, therefore read by a processor the reference to protocol context)**;

(c) storing a tunnel context based on the protocol context in said memory of the first mobile security system, wherein said tunnel context includes said at least one of the identifiers **(col. 13 lines 40-49)**; and

(d) transferring said tunnel context to the second mobile network security system thereby protecting the second mobile data network wherein the mobile station associated with said tunnel context roams to the second mobile data network**(col. 13 lines 40-49)**.

Regarding claim 23, Barnes discloses the method, according to claim 22, wherein said transferring said tunnel context occurs prior to the hand-off from the first mobile data network to the second mobile data network **(col. 13 lines 40-49)**.

Regarding claim 24, Barnes discloses a method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a

protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps off

(a) providing a mobile network security system including an interface to the mobile data network**(Fig. 4 item 264)**, a processor **(col. 4 lines 13-18, an IP security process, therefore must have a processor to process)** and a memory**(col. 15 line 23)**, wherein said mobile network security system monitors the creation**(col. 4 lines 36-41, creating tunnel)**, updating**(col. 13 lines 42-43 update**

tunnel) and destruction **(col. 15 lines26-33 IP tunnel for predetermined time therefore tunnel is destructed after predetermined time)** of the tunnel by" monitoring the signal packets,

(b) reading by a processor the reference to the protocol context of at least one of said data packets (**col. 4 lines 13-18 use security parameters index for identifying security context, therefore read by a processor the reference to protocol context)**;

Barns fails to teach step (c). **Greis** teaches policy control function which performs applying a policy based on a tunnel profile **([0025] tunnel profile such as QoS; [0026] apply a policy)**, thereby performing at least one action to said at least one of the data packets, wherein said tunnel profile is selected based on at least one of the identifiers

carried in the protocol context **([0025] distribution of packets based on TFT parameters which are included in protocol context as indicated in [0029])**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the steps taught by Greis into the method disclosed by Barnes in order to further improve the security system by applying specific policy based on the context setting.

Greis fails to teach performing action based on the payload. Albert Dobson teaches a network monitoring method and system which identifies data packets from IMSI/phone number in the payload **([0137])** which has one or more associated PDP addresses **([0138])**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the feature taught by Albert Dobson into the step disclosed by Barn and Greis in order to further enhance the security system by applying security policies based on specific user profile embedded in the payload.

Regarding claim 25, Barns discloses a program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 1 **(col. 15 lines 19-32)**.

Regarding claim 26, Barns discloses a program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 10**(col. 15 lines 19-32)**.

Regarding claim 27, Barns discloses a program storage device readable by a machine tangibly embodying a program of instructions executable-by the machine for implementing the method of claim 11**(col. 15 lines 19-32)**.

Regarding claim 28, Barns discloses a program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 22**(col. 15 lines 19-32)**.

Regarding claim 29, Barns discloses a program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 24**(col. 15 lines 19-32)**.

3. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Barnes et al. (US 6711147)**, herein after referred as Barnes, in view of **Greis (US 2004/0028034)**, further in view of **Marvit (US 6625734).**

Regarding claim 11, Barnes discloses a method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a

protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of

(a) providing a mobile network security system including an interface to the mobile data network**(Fig. 4 item 264)**, a processor **(col. 4 lines 13-18, an IP security process, therefore must have a processor to process)** and a memory**(col. 15 line 23)**, wherein said mobile network security system monitors the creation**(col. 4 lines 36-41, creating tunnel)**, updating **(col. 13 lines 42-43 update**

tunnel) and destruction **(col. 15 lines26-33 IP tunnel for predetermined time therefore tunnel is destructed after predetermined time)** of the tunnel by monitoring the signal packets **(col. 4 lines 28-42),**

Barns fails to teach step (b). Greis teaches a policy control function which performs reading by a processor the reference to the protocol context of at least one of said data packets **([0025] Data packets are treated based on PDP context therefore there must be a processor reading the protocol context)**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the steps taught by Greis into the method disclosed by Barnes in

order to further improve the security system by sending data packets based on protocol context.

Barns fails to disclose step (c). Greis teaches a policy control function that drops data packets based on PDP context ([0025]). But Greis fails to disclose the data packets are destroyed when used by an unauthorized user. **Marvit** teaches a security method that destroys data when an unauthorized user may fain access to the data **(Col. 5 lines 8-15)**. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to incorporate the data destruction taught by Marvit into the method disclosed by Barns and Greis in order to further improve the security system by destroying data when an unauthorized user is detected.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ronneke (US 2007/0226780) discloses a method relating to security in networks supporting communication of packet data.

Jouppi (US 2003/0221016) discloses a security function in packet data transmissions.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to KATHY WANG-HURST whose telephone number is

(571)270-5371. The examiner can normally be reached on Monday-Thursday, 7:30am-5pm, alternate Fridays, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Benny Tieu can be reached on (571)272-7490. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KATHY WANG-HURST/
Examiner, Art Unit 4173

/Lewis G. West/
Primary Examiner, Art Unit 2618